



# CVE-2021-32032

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-32032
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-21 04:15:00 UTC
<b>Updated</b>	2021-05-27 22:33:00 UTC
<b>Description</b>	In Trusted Firmware-M through 1.3.0, cleaning up the memory allocated for a multi-part cryptographic operation (in the event of a failure) before returning to the user.

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linaro	Trusted Firmware-m	All	All	All	All

## References

### Reference

- [crypto\\_multi\\_part\\_ops\\_abort\\_fail.rst « security\\_advisories « security « docs - trusted-firmware-m.git - Trusted Firmware for M profile Arm CPU](#)
- [Trusted Firmware - Open Source Secure Software - Trusted Firmware](#)
- [trusted-firmware-m.git - Trusted Firmware for M profile Arm CPUs](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**